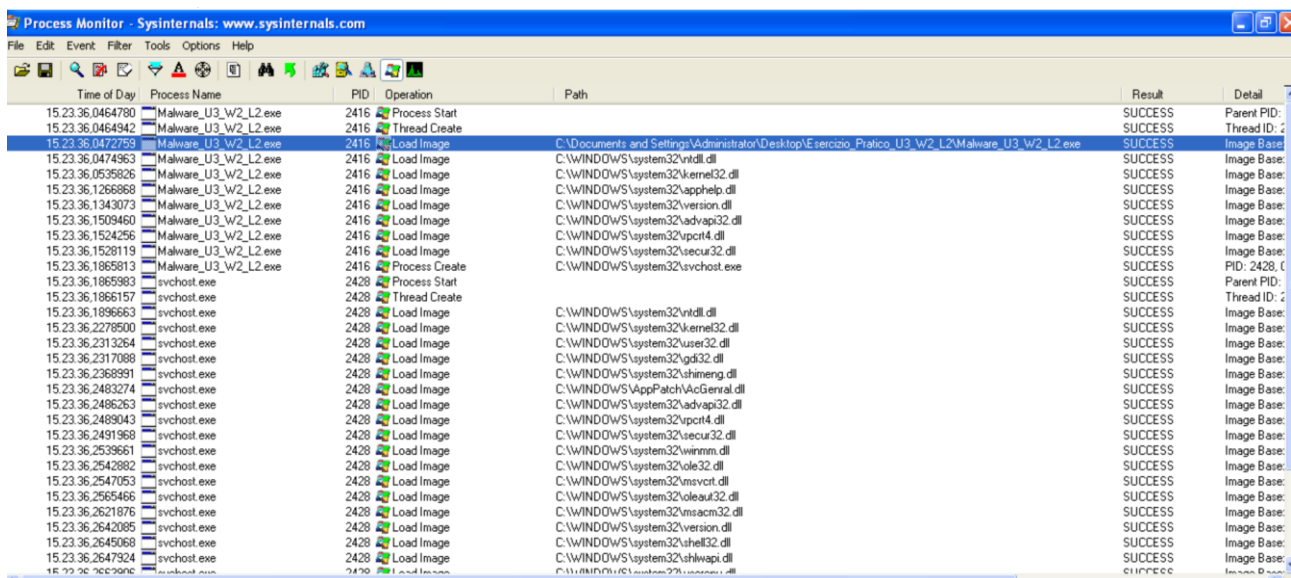


Esercizio epicode 28.11.2023

Malware analysis

Analizzare il file “Esercizio_Pratico_U3_W2_L2” con l’analisi dinamica basica



Time of Day	Process Name	PID	Operation	Path	Result	Detail
15.23.36.0464780	Malware_U3_W2_L2.exe	2416	Process Start		SUCCESS	Parent PID: 0
15.23.36.0464942	Malware_U3_W2_L2.exe	2416	Thread Create		SUCCESS	Thread ID: 2
15.23.36.0472759	Malware_U3_W2_L2.exe	2416	Load Image	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Image Base: 77D40A58
15.23.36.0474963	Malware_U3_W2_L2.exe	2416	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 77D40A58
15.23.36.0536826	Malware_U3_W2_L2.exe	2416	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 77D40A58
15.23.36.1266888	Malware_U3_W2_L2.exe	2416	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 77D40A58
15.23.36.1343073	Malware_U3_W2_L2.exe	2416	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 77D40A58
15.23.36.1509460	Malware_U3_W2_L2.exe	2416	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 77D40A58
15.23.36.1524256	Malware_U3_W2_L2.exe	2416	Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS	Image Base: 77D40A58
15.23.36.1528119	Malware_U3_W2_L2.exe	2416	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 77D40A58
15.23.36.1865813	Malware_U3_W2_L2.exe	2416	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 2428, Parent PID: 2416
15.23.36.1865983	svchost.exe	2428	Process Start		SUCCESS	Parent PID: 2416
15.23.36.1866157	svchost.exe	2428	Thread Create		SUCCESS	Thread ID: 2
15.23.36.1896663	svchost.exe	2428	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 77D40A58
15.23.36.2278500	svchost.exe	2428	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 77D40A58
15.23.36.2313264	svchost.exe	2428	Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS	Image Base: 77D40A58
15.23.36.2317088	svchost.exe	2428	Load Image	C:\WINDOWS\system32\gdi32.dll	SUCCESS	Image Base: 77D40A58
15.23.36.2368991	svchost.exe	2428	Load Image	C:\WINDOWS\system32\shimeng.dll	SUCCESS	Image Base: 77D40A58
15.23.36.2483274	svchost.exe	2428	Load Image	C:\WINDOWS\AppPatch\AcGenral.dll	SUCCESS	Image Base: 77D40A58
15.23.36.2486263	svchost.exe	2428	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 77D40A58
15.23.36.2489043	svchost.exe	2428	Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS	Image Base: 77D40A58
15.23.36.2491968	svchost.exe	2428	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 77D40A58
15.23.36.2539661	svchost.exe	2428	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 77D40A58
15.23.36.2542882	svchost.exe	2428	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 77D40A58
15.23.36.2547053	svchost.exe	2428	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 77D40A58
15.23.36.2565466	svchost.exe	2428	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 77D40A58
15.23.36.2621876	svchost.exe	2428	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 77D40A58
15.23.36.2642085	svchost.exe	2428	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 77D40A58
15.23.36.2645068	svchost.exe	2428	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 77D40A58
15.23.36.2647924	svchost.exe	2428	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 77D40A58
15.23.36.2650996	svchost.exe	2428	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 77D40A58

Grazie a procmon potremo vedere i processi e i thread che avvia una volta eseguito il file malevolo, ci soffermiamo soprattutto il process Start che esegue uno spostamento dal PID iniziale a quello di svchost, processo di sistema essenziale che si occupa nell’ospitare uno o più servizi del sistema operativo Windows.

Tramite le varie librerie importate, che possiamo visualizzare sulla path di procmon, possiamo ipotizzare che si tratta di un keylogger.

Possiamo verificarlo andando a vedere il file notepad che si è creato nella cartella in cui è presente l’eleggibile. Qualsiasi digitazione sulla tastiera viene trasposto nel file.